SECURE CONTROLS FRAMEWORK (SCF) OVERVIEW & INSTRUCTIONS

version 2024.3

con·trol
/kən trol/

A control is the power to influence or direct behaviors and the course of events. That is precisely why the Secure Controls Framework™ (SCF) was developed – we want to influence secure practices within organizations so that both cybersecurity and privacy principles are designed, implemented and managed in an efficient and sustainable manner.

NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions. For more information, please visit https://securecontrolsframework.com

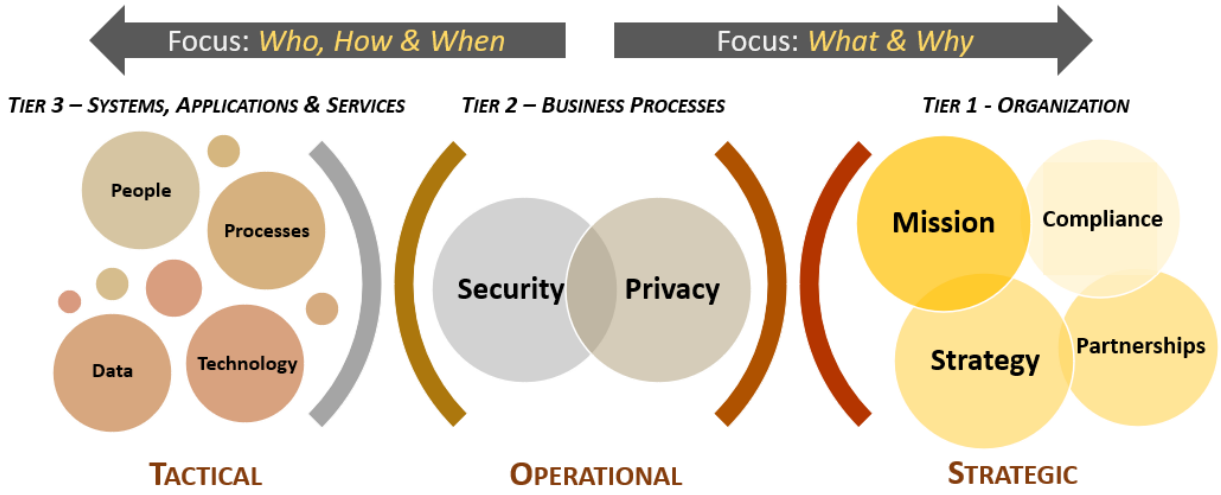
Table of Contents

EXECUTIVE SUMMARY

The Secure Controls Framework™ (SCF) focuses on internal controls. These are the cybersecurity & data privacy-related policies, standards, procedures, technologies and associated processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected. The concept is to address the broader People, Processes, Technology and Data (PPTD) that are what controls fundamentally exists to govern.

Using the SCF should be viewed as a long-term tool to not only help with compliance-related efforts but to ensure cybersecurity & data privacy principles are properly designed, implemented and maintained. The SCF helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of your data, systems, applications and other processes. The SCF can be used to assist with strategic planning down to tactical needs that impact the people, processes and technologies directly impacting your organization.

Ideally, the SCF can be used to address the "who, what where, when, why and how" for cybersecurity and data privacy at the strategic, operational and tactical levels within your organization!



This document is designed for cybersecurity & data privacy practitioners to gain an understanding of how the SCF is intended to be used in their organization.

This "best practices" guide covers the following topics:

- Level setting what the SCF is and what it is not;
- Integrated Controls Management (ICM) approach to GRC;[1]
- Leveraging the Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM);[2]
- Leveraging the Cybersecurity & Data Privacy Risk Management Model (C|P-RMM);[3] and
- Recommendations to tailor the control set for your needs to operationalize the SCF.

[1] *Integrated Controls Management (ICM) - https://securecontrolsframework.com/integrated-controls-management/*
[2] *SCF C|P-CMM - https://securecontrolsframework.com/capability-maturity-model/*
[3] *SCF C|P-RMM - https://securecontrolsframework.com/risk-management-model/*

TERMINOLOGY & ACRONYMS

The SCF Council recognizes two (2) primary sources for authoritative definitions for cybersecurity and data privacy terminology:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[4] and
- NIST Glossary.[5]

From the context of building a cybersecurity and data privacy program, it is important to clarify mandatory versus optional criteria:[6]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

TERMINOLOGY STANDARDIZATION

Within the cybersecurity profession, the term "control" can be applied to a variety of contexts and can serve multiple purposes. When used in content with the SCF, a control is a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs specified by security requirements.

- Controls are:
  - The power to make decisions about how something is managed or how something is done;
  - The ability to direct the actions of someone or something;
  - An action, method or law that limits; and/or
  - A device or mechanism used to regulate or guide the operation of a machine, apparatus or system.
- Requirements are statements that translate, or express, a need and its associated constraints and conditions.

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an organization's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire organization;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an organization; or
    - A specific country, or geographic region, of the organization's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. [7]
- Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. See Appendix A: Material Controls for examples of material controls. A material control is such a fundamental cybersecurity and/or data privacy control that:
  - It is not capable of having compensating controls; and
  - Its absence, or failure, exposes an organization to such a degree that it could have a material impact.
- Material Risk. When an identified risk that poses a material impact, that is a material risk.

---

[4] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[5] *NIST Glossary - https://csrc.nist.gov/glossary*
[6] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*
[7] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*

    - A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
    - A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.
- Material Threat. When an identified threat poses a material impact, that is a material threat.
    - A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
    - A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.
- Material Incident. When an incident poses a material impact, that is a material incident.
    - A material incident is an occurrence that does or has the potential to:
        - Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
        - Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).
    - Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate practices to identify, respond to and recover from such incidents.
- Material Weakness. A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.
    - When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable the timely identification and response to incidents, etc.).
    - A material weakness will be identified as part of a gap assessment, audit or other form of assessment as a finding due to one (1), or more, control deficiencies. A material weakness should be documented in an organization's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism for remediation purposes.
- Reciprocity. Reciprocity is an agreement among participating organizations to accept each other's: [8]
    - Security assessments to reuse system resources; and/or
    - Assessed security posture to share information.
- Risk. A risk is:
    - A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or
    - To expose someone or something valued to danger, harm or loss (verb).
- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.[9]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result. [10]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.[11]
- Threat. A threat:
    - Is a person, or thing, likely to cause damage or danger (noun); or
    - Indicates impending damage or danger (verb).

[8] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*
[9] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[10] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[11] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*

ACRONYMS

The following acronyms are defined as:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations (e.g., internal assessments).
3PA	Third-Party Attestation	3PA are attestations made by an independent third-party, generally in the performance of an assessment or audit.
3PAAC	Third-Party Assessment, Attestation and Certification Services	Assessment, attestation and certification services performed by a third-party organization.
3PAO	Third-Party Assessment Organization	A company that performs assessment, attestation and certification services.
AAT	Artificial Intelligence and Autonomous Technologies	Tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
AO	Assessment Objective	AOs are objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.
APIT	Automated Point In Time	APIT assessments utilize automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence: ▪ Relevant to a specific point in time (time at which the control was evaluated); ▪ In situations where technology cannot evaluate evidence, evidence is manually reviewed; and ▪ The combined output of automated and manual reviews of artifacts is used to derive a finding.
ATE	Assessment Technical Expert	ATE are assessment team members who have the necessary subject matters expertise to conduct a specific part of an assessment. ATE report to the ATL.
ATL	Assessment Team Lead	An ATL is an individual assigned by the 3PAO to lead its assessment team in the conduct of 3PAAC Services.
AEHR	Automated Evidence with Human Assessment	AEHR assessments are used for ongoing, continuous control assessments: ▪ AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and ▪ Recurring human reviews: ○ Evaluate the legitimacy of the results from automated control assessments; and ○ Validate the automated evidence review process to derive a finding.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
COI	Conflict of Interest	COI involves situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
CPE	Continuing Professional Education	CPE describes the ongoing process of improving skills and competencies through formal or informal educational activities.
DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data privacy controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the organization's respective industry and risk tolerance.
ERL	Evidence Request List	ERLs establish a finite list of supporting evidence used in an assessment: ▪ Prior to the start of the assessment, an ERL is provided by the 3PAO to the OSA. ▪ The ERL's standardized evidence expectations allow OSAs to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.
ESP	External Service Provider	An independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting / professional services;

		▪ Software development; ▪ Staff augmentation; and ▪ Technology support (e.g., Managed Services Provider (MSP)).
MCR	Minimum Compliance Requirements	MCR are minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.
MPIT	Manual Point In Time	MPIT assessments are a traditional assessment methodology: ▪ Relevant to a specific point in time (time at which the control was evaluated); and ▪ Relies on the manual review of artifacts to derive a finding.
MLC	Maturity Level Criteria	MLC are specific to each maturity level to define reasonable staffing, technologies and processes to implement the desired level of maturity.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
OSA	Organization Seeking Assessment	A company, entity or business unit seeking the external assessment.
PbD	Privacy by Design	Data protection through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
ROC	Report on Conformity	A formalized report that issues an assessment conformity designation. The ROC summarizes the assessment findings and justification for the conformity designation.
SbD	Secure by Design	Processes and technologies are designed and built in a way that protects against reasonable threats. SbD prioritizes cybersecurity as a core business requirement, rather than treating it as a technical feature.
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).

SECTION 1: UNDERSTANDING THE SCF

It is important for users of the SCF to understand what the SCF is and what it is not. We are very transparent on what the SCF offers and we want to help ensure that SCF users understand their role in using the SCF in their efforts to secure their organization.

WHY SHOULD I USE THE SCF?

There is no sales pitch for using the SCF – it is a free resource so there is no financial incentive for us to make companies use it. For companies that have just one 1-2 compliance requirements, the SCF might be considered overkill for your needs. However, for companies that have 3+ compliance requirements (e.g., organization that has requirements to address ISO 27002, SOC 2, PCI DSS and GDPR), then the SCF is a great tool to streamline the management of cybersecurity & data privacy controls.

In developing the SCF, we identified and analyzed over 100 statutory, regulatory and contractual frameworks. Through analyzing these thousands of legal, regulatory and framework requirements, we identified commonalities and this allows several thousand unique controls to be addressed by approximately 1,100 controls that makeup the SCF. For instance, a requirement to maintain strong passwords is not unique, since it is required by dozens of laws, regulations and frameworks. This allows one well-worded SCF control to address multiple requirements. This focus on simplicity and sustainability is key to the SCF, since it can enable various teams to speak the same controls language, even though they may have entirely different statutory, regulatory or contractual obligations that they are working towards.

The SCF targets silos, since siloed practices within any organization are inefficient and can lead to poor security, due to poor communications and incorrect assumptions.

Some people freak out and think they have to do 1,000+ controls in the SCF and that is just not the case. It is best to visualize the SCF as a "buffet of cybersecurity & data privacy controls," where there is a selection of 1,000+ controls available to you. Just as you do not eat everything possible on a buffet table, the same applies to the SCF's control set. Once you know what is applicable to you, you can generate a customized control set that gives you just the controls you need to address your statutory, regulatory and contractual obligations.

WHAT THE SCF IS

The SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications. The SCF addresses both cybersecurity & data privacy, so that these principles are designed to be "baked in" at the strategic, operational and tactical levels.

The SCF is:

- A control set
- A useful tool to provide a "Rosetta Stone" approach to organizing cybersecurity & data privacy controls so that the same controls can be used among companies and teams (e.g., privacy, cybersecurity, IT, project, procurement, etc.).
- Free for businesses to use. A result of a volunteer-led effort that uses "expert derived assessments" to perform the mapping from the controls to applicable laws, regulations and other frameworks.

The SCF also contains helpful guidance on possible tools and solutions to address controls. Additionally, it contains maturity criteria that can help an organization plan for and evaluate controls, based on a target maturity level.

WHAT THE SCF IS NOT

While the SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications, the SCF will only ever be a control set and is not a "magic bullet" technology solution to address every possible cybersecurity & data privacy compliance obligation that an organization faces.

The SCF is not:

- A substitute for performing due diligence and due care to understand and manage your specific compliance needs.
- A complete technology or documentation solution to address all your cybersecurity & data privacy needs (e.g., the policies, standards, procedures and processes you need to have in place to be secure and compliant).
- Infallible or guaranteed to meet every compliance requirement your organization offers, since the controls are mapped

based on expert-derived assessments to provide the control crosswalking that relies on human expertise and that is not infallible.

Designing & Building An Audit-Ready Cybersecurity & Data Privacy Program

Building an audit-ready cybersecurity & data privacy program requires addressing the holistic nature of cybersecurity & data privacy concerning how people, processes and technology impact security practices.

Building a security program that routinely incorporates cybersecurity & data privacy practices into daily operations requires a mastery of the basics. A useful analogy is with the children's toy, LEGO®. With LEGO® you can build nearly anything you want — either through following directions or using your own creativity. However, it first requires an understanding of how various LEGO® shapes either snap together or are incompatible.

Once you master the fundamentals with LEGO®, it is easy to keep building and become immensely creative since you know how everything interacts. However, when the fundamentals are ignored, the LEGO® structure will be weak and include systemic flaws. Security and privacy really are not much different, since those disciplines are made up of numerous building blocks that all come together to build secure systems and processes. The lack of critical building blocks will lead to insecure and poorly architected solutions.

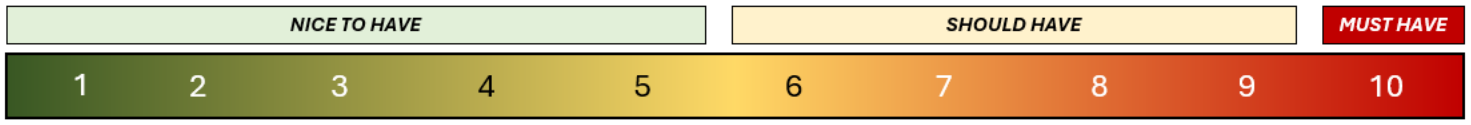
When you envision each component that makes up a security or privacy "best practice" is a LEGO® block, it is possible to conceptualize how certain requirements are the foundation that form the basis for other components to attach to. Only when all the building blocks come together and take shape do you get a functional security / privacy program!

Think of the SCF as a toolkit for you to build out your overall security program domain-by-domain so that cybersecurity & data privacy principles are designed, implemented and managed by default!

SCF Control Weighting Explanation

The SCF assigns a value on a scale from 1-10, with 1 being the least important and 10 being the most important. These values are subjective, based on SCF contributor discussion, since control weighting is important to help prioritize controls and assist with the understanding what really matters from a risk management perspective. For an insight into the thought process, a control weighting of 10 was framed as *"Would you do business with an organization that did not have this control in place?"* where certain controls were identified as an absolute minimum from a risk threshold perspective from a "reasonable person" perspective.

- Those controls designated as a score of **10** should be considered a **MATERIAL / KEY CONTROL** (e.g., lack of or a deficiency should be considered a material weakness).
- On the opposite site of the spectrum, a score of **1** was deemed **"nice to have"** but did not materially affect risk.



Note: The intended usage of materiality is meant to provide relevant context regarding risk thresholds. Materiality designations are intended to act as a "guard rail" for risk management decisions. A material weakness crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

A financial benchmark is commonly used to determine materiality. From a financial impact perspective, for an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one, or more, of the following criteria where the potential financial impact is measured as:[12]

- *≥ 5% of pre-tax income*
- *≥ 0.5% of total assets*
- *≥ 1% of total equity (shareholder value); and/or*
- *≥ 0.5% of total revenue.*

[12] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*

Tailoring Is Required - Not All SCF Controls Are Applicable To Your Organization

Please keep in mind that the SCF is a tool and it is only as good as how it is used – just like a pocketknife shouldn't be used as a prybar. Realistically, if you do not scope the controls from the SCF correctly, you will not address your applicable compliance requirements since you are missing what is expected. That is not a deficiency of the SCF – that is simply negligence on the part of the user of the tool.

To make sure scoping is done properly, it is imperative for you to speak with your legal, IT, project management, cybersecurity and procurement teams. The reason for this collaboration is so that you can get a complete picture of all the applicable laws, regulations and frameworks that your organization is legally obligated to comply with. Those teams will likely provide the best insights into what is required and that list of requirements will then make it simple to go through and customize the SCF for your specific needs!

Understanding the requirements for both cybersecurity & data privacy principles involves a simple process of distilling expectations. This process is all part of documenting reasonable expectations that are "right-sized" for an organization, since every organization has unique requirements.

Beyond just using compliance terminology properly, understanding which of the three types of compliance is crucial in managing both cybersecurity & data privacy risk within an organization. The difference between non-compliance can be as stark as (1) going to jail, (2) getting fined, (3) getting sued, (4) losing a contract or (5) an unpleasant combination of the previous options.

Understanding the "hierarchy of pain" with compliance leads to well-informed risk decisions that influence technology purchases, staffing resources and management involvement. That is why it serves both cybersecurity and IT professionals well to understand the compliance landscape for their benefit, since you can present issues of non-compliance in a compelling business context to get the resources you need to do your job.

The most common types of compliance requirements are:

1. Statutory
2. Regulatory
3. Contractual

Statutory Requirements

Statutory obligations are required by law and refer to current laws that were passed by a state or federal government. These laws are generally static and rarely change unless a new law is passed that updates it, such as the HITECH Act, which provided updates to the two-decades-old HIPAA.

From a cybersecurity & data privacy perspective, statutory compliance requirements include:

- **US – Federal Laws**
  - Children's Online Privacy Protection Act (COPPA)
  - Fair and Accurate Credit Transactions Act (FACTA) – including "Red Flags" rule
  - Family Education Rights and Privacy Act (FERPA)
  - Federal Information Security Management Act (FISMA)
  - Federal Trade Commission (FTC) Act
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA) / HITECH Act
  - Sarbanes-Oxley Act (SOX)
- **US – State Laws**
  - California SB1386
  - Massachusetts 201 CMR 17.00
  - Oregon ORS 646A.622
- **International Laws**
  - Canada – Personal Information Protection and Electronic Documents Act (PIPEDA)
  - UK – Data Protection Act (DPA)
  - Other countries' variations of Personal Data Protect Acts (PDPA)

Regulatory Requirements

Regulatory obligations are required by law, but they are different from statutory requirements in that these requirements refer to rules issued by a regulating body that is appointed by a state or federal government. These are legal requirements through proxy, where the regulating body is the source of the requirement. It is important to keep in mind that regulatory requirements tend to change more often than statutory requirements.

From a cybersecurity & data privacy perspective, regulatory compliance examples include:

- **US Regulations**
  - Defense Federal Acquisition Regulation Supplement (DFARS) (NIST 800-171)
  - Federal Acquisition Regulation (FAR)
  - Federal Risk and Authorization Management Program (FedRAMP)
  - DoD Information Assurance Risk Management Framework (DIARMF)
  - National Industrial Security Program Operating Manual (NISPOM)
  - New York Department of Financial Services 23 NYCRR 500
- **International Regulations**
  - European Union General Data Protection Regulation (EU GDPR)

Contractual Requirements

Contractual obligations are required by legal contract between private parties. This may be as simple as a cybersecurity or privacy addendum in a vendor contract that calls out unique requirements. It also includes broader requirements from an industry association that membership brings certain obligations.

From a cybersecurity & data privacy perspective, common contractual compliance requirements include:

- Payment Card Industry Data Security Standard (PCI DSS)
- Service Organization Control (SOC)
- Generally Accepted Privacy Principles (GAPP)
- Center for Internet Security (CIS) Critical Security Controls (CSC)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

Set Theory Relationship Mapping (STRM)

Starting in 2024, the SCF began leverages the Set Theory Relationship Mapping (STRM) for crosswalk mapping. STRM is generally well-suited to evaluate cybersecurity and data privacy laws, regulations and frameworks. With the publishing of NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings* it establishes the US Government's playbook for how to perform crosswalk mapping between different cybersecurity and data privacy laws, regulations and frameworks.[13] This document is part of NIST's broader NIST OLIR Program that is an "effort to facilitate Subject Matter Experts (SMEs) in defining standardized online informative references (OLIRs) between elements of their documents, products, and services and elements of NIST documents…" The SCF currently participates in the National Online Informative References (OLIR) Program and with NIST's preference for STRM, we decided an aligned crosswalk mapping methodology makes sense.

For SCF's STRM practices, the SCF is always the "reference document" and the law, regulation or framework being mapped to is always the "focal document."

REFERENCE DOCUMENT (RD)

FOCAL DOCUMENT (FD)

[13] *NIST IR 8477* - https://csrc.nist.gov/pubs/ir/8477/final

STRM Relationship Type #1: SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

STRM Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

STRM Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

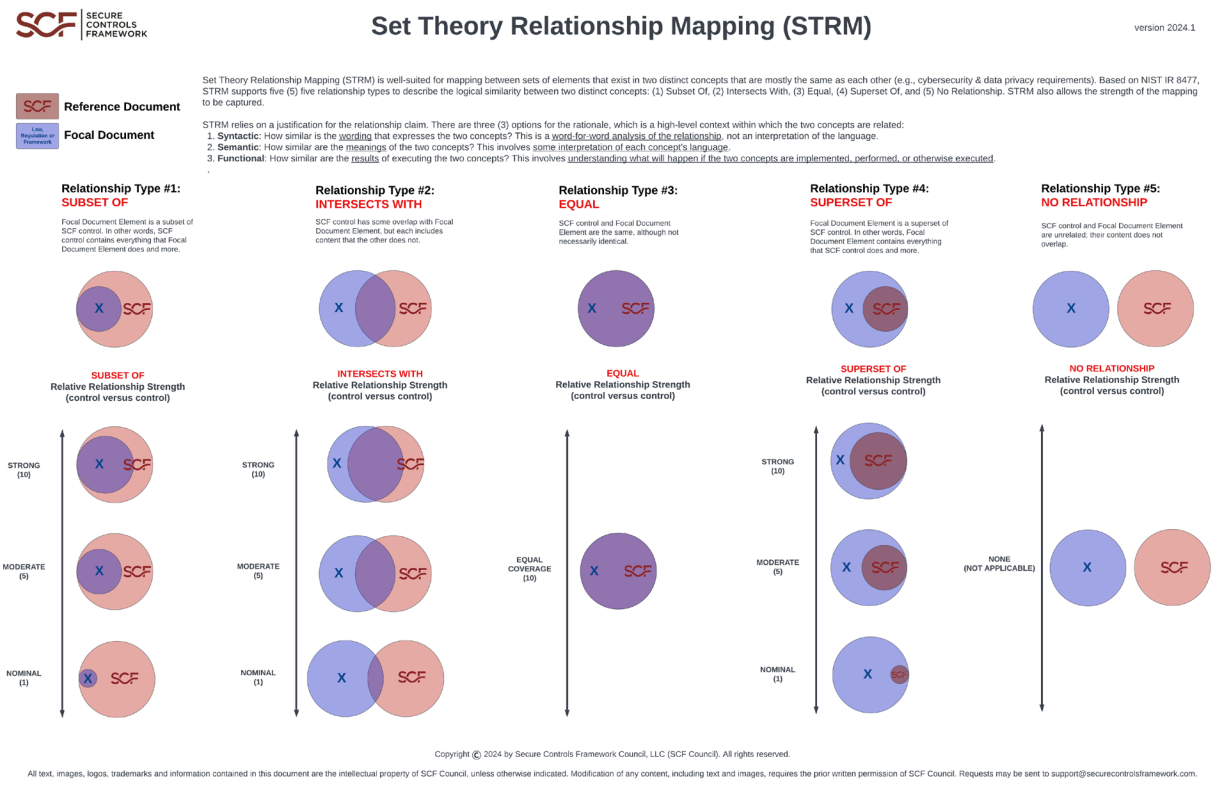
STRM Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

STRM Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.

These can be viewed at: https://securecontrolsframework.com/content/strm/scf-set-theory-relationship-mapping.pdf



Expert-Derived Content (EDC) vs Natural Language Processing (NLP)

What NIST IR 8477 does is provide the "gold standard" practice for how an individual can perform crosswalk mapping with no technology needed, where it can literally be performed with a pencil and piece of paper. Children learn the process of diagramming sentences in grade school (e.g., Reed–Kellogg model) with pencils and paper. This is the process of graphically identifying nouns, verbs, adjectives and modifiers to teach proper sentence structure for how various components of language work together to communicate an idea. With the advent of Artificial Intelligence (AI), the ability to diagram sentences in both computer and human-readable format is achievable through Natural Language Processing (NLP). From a cybersecurity crosswalking perspective, NLP can be used to evaluate a control statement (e.g., must have firewall) to identify the noun (e.g., firewall) and verb (e.g., must have) to determine the relative strength it maps to a different control (e.g., shall have network defense appliances). Where that becomes interesting is both in protecting the underlying content (e.g., Intellectual Property (IP)) and patentability.

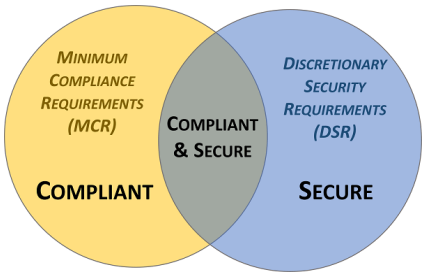
While the SCF leverages expert-derived content (e.g., human subject-matter experts), other solutions use NLP to create their crosswalk mapping. One significant downside for those solutions leveraging NLP is their forfeit of IP since AI-generated content is currently prohibited from copyright protections due to the content not being the work of a human creator. Therefore, NLP-generated content could be considered free content from an IP perspective, since a copyright of AI-generated content would not be enforceable.

Where it gets even more fascinating with AI-based solutions in the compliance space is with patentability for inventions due to the "mental steps" doctrine. In 2014, the US Supreme Court ruled that inventions are ineligible for patenting if the patent claim is something a human could do in their mind or with paper and pencil (e.g., a human performing sentence diagramming on a piece of paper and comparing the results of that sentence diagram with another). That landmark case (*Alice Corp. v. CLS Bank International*) established a new uncertainty about patent eligibility of AI and machine learning technologies. The result of Alice is that patents issued for compliance solutions leveraging NLP to perform crosswalk mapping may not hold up to scrutiny by the Patent Trial and Appeal Board (PTAB) given NIST published a document that describes how to perform crosswalk mapping without the assistance of technology.

SECTION 2: DEFINING WHAT IT MEANS TO BE "SECURE & COMPLIANT"

It is important to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, an organization needs to categorize its applicable controls according to "must have" vs "nice to have" requirements:

- **Minimum Compliance Requirements (MCR)** are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- **Discretionary Security Requirements (DSR)** are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity & data privacy controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.



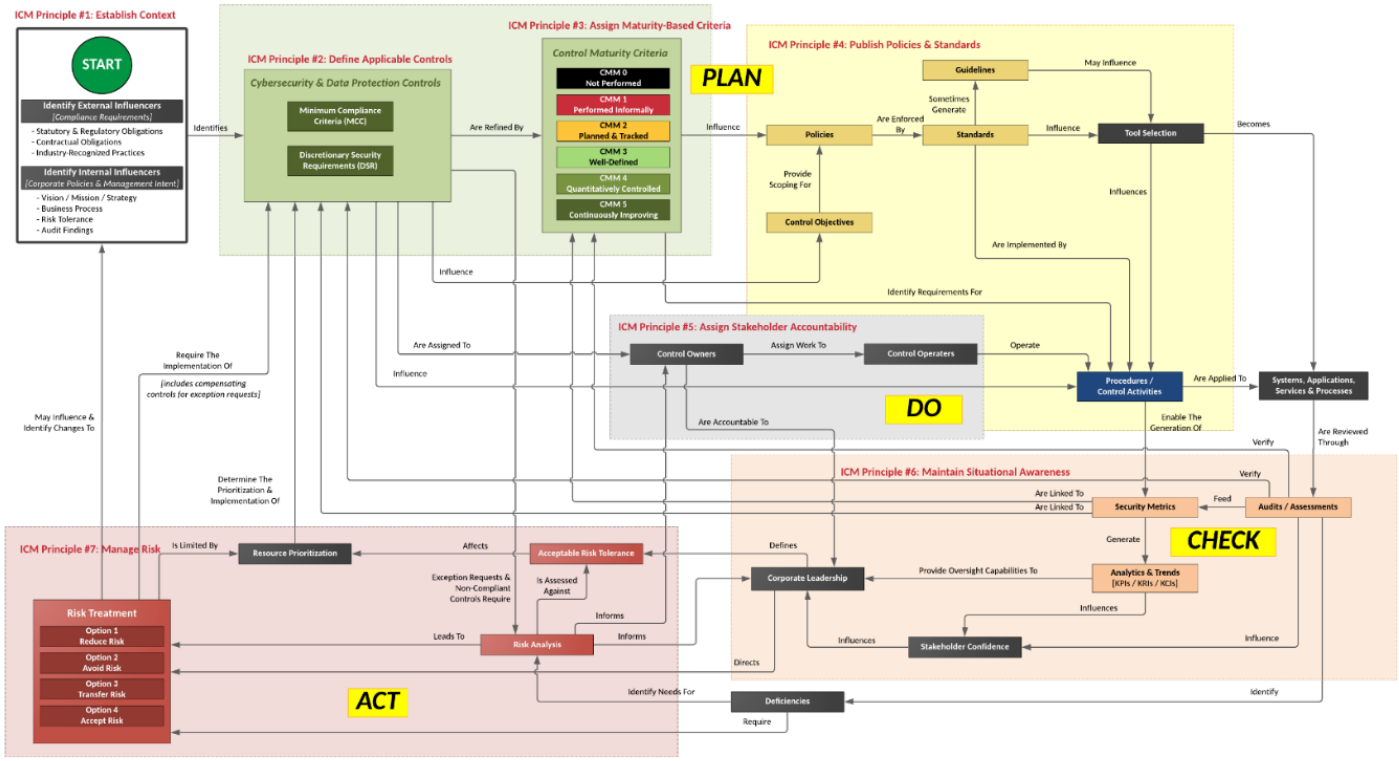
Secure and compliant operations exist when both MCR and DSR are implemented and properly governed:

- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

ComplianceForge helped develop the Integrated Controls Management (ICM) model to help streamline the traditional "governance, risk management & compliance" functions. There are eight (8) principles associated with ICM:

1. Establish Context
2. Define Applicable Controls
3. Assign Maturity-Based Criteria
4. Publish Policies, Standards & Procedures
5. Assign Stakeholder Accountability
6. Maintain Situational Awareness
7. Manage Risk
8. Evolve Processes

The ICM is very much worth your time to familiarize yourself with: https://www.complianceforge.com/grc/integrated-controls-management/



[graphic can be downloaded from https://complianceforge.com/content/Plan-Do-Check-Act.pdf]

Section 3: Understanding What It Means To Adopt "Secure by Design" Principles

For an organization that just "does" ISO 27002, it is easy to say, "We're an ISO shop and we exclusively use ISO 27002 cybersecurity principles" and that would be routinely accepted as being adequate. However, what about companies that have complex cybersecurity and compliance needs, such as a company that has to address SOC2, ISO 27002, CCPA, EU GDPR, PCI DSS and NY DFS? In these complex cases that involve multiple frameworks, ISO 27002 principles alone do not cut it. This is why it is important to understand what secure principles your organization is aligned with, so that the controls it implements are appropriate to build secure and compliant processes. What works for one company or industry does not necessarily work for another, since requirements are unique to the organization.

Most companies have requirements to document cybersecurity & data privacy processes, but lack the knowledge and experience to undertake such documentation efforts. That means organizations are faced with either outsourcing the work to expensive consultants or they ignore the requirement and hope they do not get in trouble for being non-compliant. In either situation, it is not a good place to be.

Secure Practices Are Common Expectations

While the European Union General Data Protection Regulation (EU GDPR) made headlines for requiring organizations to demonstrate cybersecurity & data privacy principles are by both "by default and by design," Secure Engineering & Data Privacy (SEDP) principles are not just limited to EU GDPR. SEDP principles are actually common requirements in the constantly-evolving statutory and regulatory landscapes. The following are common statutory, regulatory and contractual requirements that expect SEDP practices:

- AICPA Trust Services Principles (TSP) (e.g., System and Organization Controls (SOC) 2 Type 1) – CC2.2, CC3.2, CC5.1 & CC5.2
- Cloud Computing Compliance Controls Catalogue (C5) – KOS-01 & KOS-07
- Criminal Justice Information Services (CJIS) Security Policy – 5.10.1.1 & 5.10.1.5
- COBIT 2019 – DSS06.06
- COSO 2017 – Principles 10 & 11
- European Union Agency for Network and Information Security (ENISA) Technical Guideline of Security Measures – SO12
- European Union General Data Protection Regulation (EU GDPR) – Art 5.2, 24.1, 24.2, 24.3, 25.1, 25.2, 25.3, 32.1, 32.2 & 40.2
- Federal Risk and Authorization Management Program (FedRAMP) – SA-8, SC-7(18) & SI-01
- Food & Drug Administration (FDA) 21 CFR Part 11 – §11.30
- Federal Trade Commission (FTC) Act - §45(a) & §45b(d)(1)
- Generally Accepted Privacy Principles (GAPP) – 4.2.3, 6.2.2, 7.2.2 & 7.2.3
- Health Insurance Portability and Accountability Act (HIPAA) - 164.306, 164.308, 164.312, 164.314 & 164.530
- ISO 27002:2013 – 8.3.2
- ISO 27018 – A.10.1, A.10.4, A.10.5 & A.10.6
- ISO 29100 – 5.10 & 5.11
- National Industry Security Program Operating Manual (NISPOM) – 8-101, 8-302 & 8-311
- NIST SP 800-53 – PT-1, SA-8, SA-13, SC-7(18) & SI-1
- NIST SP 800-171 – 3.13.1, 3.13.3 & Non-Federal Organization (NFO)
- NIST Cybersecurity Framework – PR.IP-1
- Payment Card Industry Data Security Standard (PCI DSS) – 1.2, 1.3, 1.4, 1.5, 2.2, 6.5 & 12.5

Compliance Should Be Viewed As A Natural Byproduct of Secure Practices

It is vitally important for any SCF user to understand that "compliant" does not mean "secure." However, if you design, build and maintain secure systems, applications and processes, then compliance will be a natural byproduct of those secure practices.

The SCF's comprehensive listing of over 1,000 cybersecurity & data privacy controls is categorized into thirty-three (33) domains that are mapped to over 110 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the cybersecurity & data privacy principles to help an organization ensure that secure practices are implemented by design and by default.

You may be asking yourself, "What cybersecurity & data privacy principles should I be using?" and that is a great question. The SCF helped with this common question by taking the thirty-three (33) of the SCF and creating principles that an organization can use. The idea is that by focusing on these secure principles, an organization will design, implement and maintain secure systems, applications and processes that will by default help the organization comply with its compliance obligations.

Cybersecurity & Data Privacy by Design (C|P) Principles

The concept of building cybersecurity & data privacy into technology solutions both by default and by design is a basic expectation for businesses, regardless of the industry. The adoption of cybersecurity & data privacy principles is a crucial step in building a secure, audit-ready program.

The C|P is a set of thirty-three (33) cybersecurity & data privacy principles that leverage the SCF's extensive cybersecurity & data privacy control set. You can download the free poster at https://securecontrolsframework.com/domains-principles/.

The "C pipe P" logo is a nod to the computing definition of the | or "pipe" symbol (e.g., shift + backslash), which is a computer command line mechanism that allows the output of one process to be used as input to another process. In this way, a series of commands can be linked to more quickly and easily perform complex, multi-stage processing. Essentially, the concept is that security principles are being "piped" with privacy principles to create secure processes in an efficient manner.

Steps To Operationalize The C|P Principles

1. Read through the C|P principles to familiarize yourself with the thirty-three (33) to understand how they come together to address the cybersecurity, privacy and physical security considerations for a modern security program.
2. Identify the applicable SCF controls that your organization needs to implement to address its applicable statutory, regulatory and contractual compliance needs.
3. Implement and monitor those SCF controls to ensure the C|P principles are being met by your day-to-day practices.

The C|P establishes thirty-three (33) common-sense principles to guide the development and oversight of a modern cybersecurity & data privacy program. Those thirty-three (33) C|P principles are listed below:

SCF Domains & C|P Principles

#	SCF Domain	SCF Identifier	Cybersecurity & Data Privacy by Design (C|P) Principles	Principle Intent
1	Cybersecurity & Data Privacy Governance	GOV	Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data privacy principles that address applicable statutory, regulatory and contractual obligations.	Organizations specify the development of an organization's cybersecurity & data privacy programs, including criteria to measure success, to ensure ongoing leadership engagement and risk management.
2	Artificial and Autonomous Technology	AAT	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.	Organizations ensure Artificial Intelligence (AI) and autonomous technologies are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced. In addition, AI-related risks are governed according to technology-specific considerations to minimize emergent properties or unintended consequences.
3	Asset Management	AST	Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.	Organizations ensure technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal, ensuring only authorized devices are allowed to access the organization's network and to protect the organization's data that is stored, processed or transmitted on its assets.
4	Business Continuity & Disaster Recovery	BCD	Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.	Organizations establish processes that will help the organization recover from adverse situations with minimal impact to operations, as well as provide the capability for e-discovery.

5	Capacity & Performance Planning	CAP	Govern the current and future capacities and performance of technology assets.	Organizations prevent avoidable business interruptions caused by capacity and performance limitations by proactively planning for growth and forecasting, as well as requiring both technology and business leadership to maintain situational awareness of current and future performance.
6	Change Management	CHG	Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.	Organizations ensure both technology and business leadership proactively manage change, including the assessment, authorization and monitoring of technical changes across the enterprise so as to not impact production systems uptime and allow easier troubleshooting of issues.
7	Cloud Security	CLD	Govern cloud instances as an extension of on-premises technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.	Organizations govern the use of private and public cloud environments (e.g., IaaS, PaaS and SaaS) to holistically manage risks associated with third-party involvement and architectural decisions, as well as to ensure the portability of data to change cloud providers, if needed.
8	Compliance	CPL	Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.	Organizations ensure controls are in place to ensure adherence to applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.
9	Configuration Management	CFG	Enforce secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.	Organizations establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features can be inadvertently or deliberately omitted or rendered inoperable, allowing processing irregularities to occur or the execution of malicious code.
10	Continuous Monitoring	MON	Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.	Organizations establish and maintain ongoing situational awareness across the enterprise through the centralized collection and review of security-related event logs. Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the organization will have "blind spots" in its situational awareness that could lead to system compromise, data exfiltration, or unavailability of needed computing resources.
11	Cryptographic Protections	CRY	Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.	Organizations ensure the confidentiality and integrity of its data through implementing appropriate cryptographic technologies to protect systems, applications, services and data.

12	Data Classification & Handling	DCH	Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.	Organizations ensure that technology assets, both electronic and physical, are properly classified and measures implemented to protect the organization's data from unauthorized disclosure, or modification, regardless of if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity and availability of data.
13	Embedded Technology	EMB	Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.	Organizations specify the development, proactive management and ongoing review of security embedded technologies, including hardening of the "stack" from the hardware, firmware and software to transmission and service protocols used for Internet of Things (IoT) and Operational Technology (OT) devices.
14	Endpoint Security	END	Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.	Organizations ensure that endpoint devices are appropriately protected from security threats to the device and its data. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity, availability and safety considerations.
15	Human Resources Security	HRS	Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.	Organizations create a cybersecurity & data privacy-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.
16	Identification & Authentication	IAC	Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.	Organizations implement the concept of "least privilege" through limiting access to the organization's systems and data to authorized users only.
17	Incident Response	IRO	Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).	Organizations establish and maintain a viable and tested capability to respond to cybersecurity or data privacy-related incidents in a timely manner, where organizational personnel understand how to detect and report potential incidents.
18	Information Assurance	IAO	Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.	Organizations ensure the adequacy of cybersecurity & data privacy controls in development, testing and production environments.

19	Maintenance	MNT	Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.	Organizations ensure that technology assets are properly maintained to ensure continued performance and effectiveness. Maintenance processes apply additional scrutiny to the security of end-of-life or unsupported assets.
20	Mobile Device Management	MDM	Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.	Organizations govern risks associated with mobile devices, regardless of ownership (organization-owned, employee-owned or third-party owned). Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.
21	Network Security	NET	Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.	Organizations ensure sufficient cybersecurity & data privacy controls are architected to protect the confidentiality, integrity, availability and safety of the organization's network infrastructure, as well as to provide situational awareness of activity on the organization's networks.
22	Physical & Environmental Security	PES	Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.	Organizations minimize physical access to the organization's systems and data by addressing applicable physical security controls and ensuring that appropriate environmental controls are in place and continuously monitored to ensure equipment does not fail due to environmental threats.
23	Data Privacy	PRI	Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.	Organizations align data privacy engineering decisions with the organization's overall data privacy strategy and industry-recognized leading practices to secure Personal Data (PD) that implements the concept of data privacy by design and by default.
24	Project & Resource Management	PRM	Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.	Organizations ensure that security-related projects have both resource and project/program management support to ensure successful project execution.
25	Risk Management	RSK	Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.	Organizations ensure that the business unit(s) that own the assets and / or processes involved are made aware of and understand all applicable cybersecurity & data privacy-related risks. The cybersecurity & data privacy teams advise and educate on risk management matters, while it is the business units and other key stakeholders that ultimately own the risk.
26	Secure Engineering & Architecture	SEA	Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.	Organizations align cybersecurity engineering and architecture decisions with the organization's overall technology architectural strategy and industry-recognized leading practices to secure networked environments.

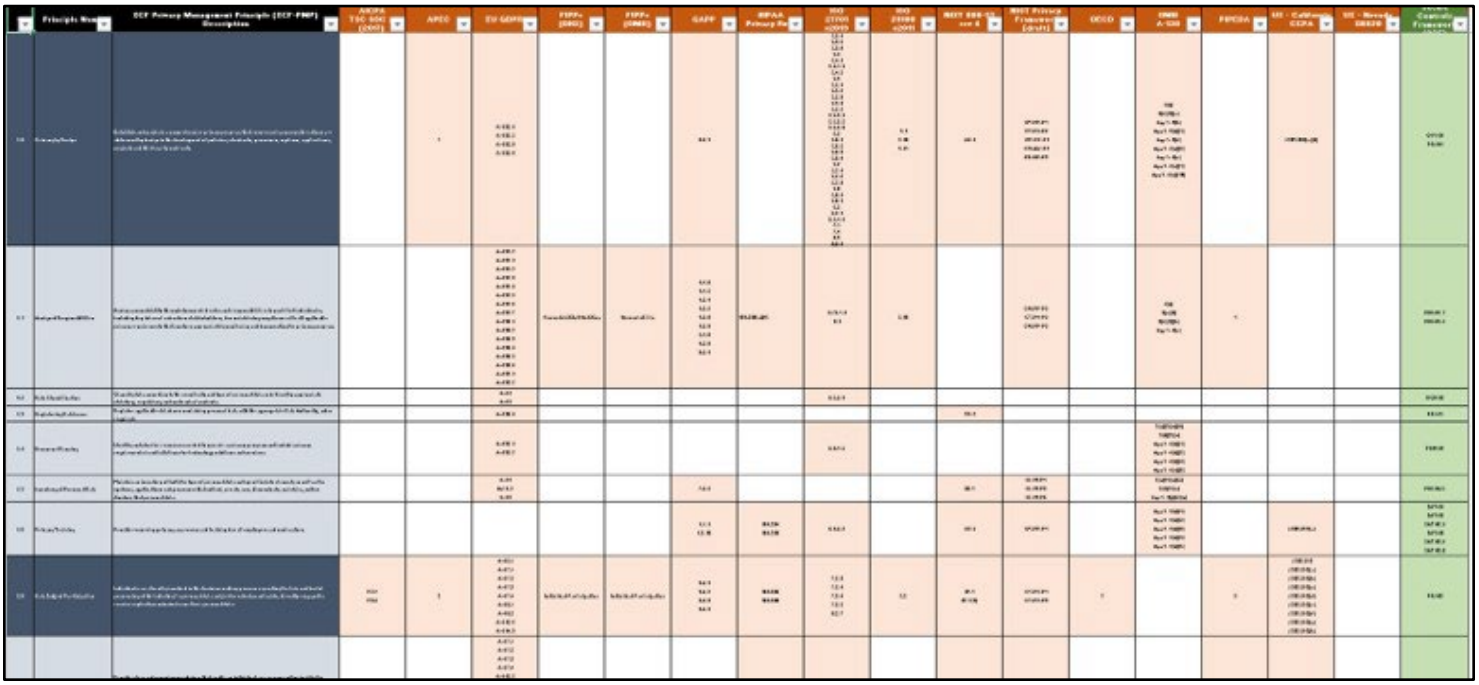
27	Security Operations	OPS	Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.	Organizations ensure appropriate resources and a management structure exist to enable the service delivery of cybersecurity, physical security and data privacy operations.
28	Security Awareness & Training	SAT	Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.	Organizations develop a cybersecurity & data privacy-minded workforce through continuous education activities and practical exercises.
29	Technology Development & Acquisition	TDA	Develop and test systems, applications or services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses.	Organizations ensure that cybersecurity & data privacy principles are implemented into any products/solutions, either developed internally or acquired, to make sure that the concepts of “least privilege” and “least functionality” are incorporated.
30	Third-Party Management	TPM	Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.	Organizations ensure that cybersecurity & data privacy risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become compromised, untrustworthy or defunct.
31	Threat Management	THR	Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.	Organizations establish a capability to proactively identify and manage technology-related threats to the cybersecurity & data privacy of the organization’s systems, data and business processes.
32	Vulnerability & Patch Management	VPM	Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.	Organizations proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.
33	Web Security	WEB	Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.	Organizations address the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing, and monitoring for malicious activities.

SECTION 4: UNDERSTANDING WHAT IT MEANS TO ADOPT "PRIVACY BY DESIGN" PRINCIPLES

Through our interactions with organizations, we identified that many organizations understand the cybersecurity framework they wanted or needed to align with, but had no understanding of the privacy principles their organization should be aligned with. We set out to fix that issue and what we did was select over a dozen of the most common privacy frameworks to create a "best in class" approach to managing privacy principles. The best part is these are all mapped to the SCF and are built into the SCF, so you can leverage the SCF for both your cybersecurity & data privacy needs!

Why should you care? When you tie the broader C|P in with the SCF Data Privacy Management Principles (DPMP), you have an excellent foundation for building and maintaining secure systems, applications and services that address cybersecurity & data privacy considerations by default and by design. The DPMP is included in the SCF download as a separate tab in the Excel spreadsheet.[14]

Think of the SCF Privacy Management Principles as a supplement to the C|P to assist in defining and managing privacy principles, based on selected privacy frameworks. This can enable your organization to align with multiple privacy frameworks that also map to your cybersecurity & data privacy control set, since we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy practitioners to comprehend.



DATA PRIVACY PRACTICES ARE COMMON EXPECTATIONS

For organizations, we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy lawyers to understand. What this project did was identify a dozen of the leading privacy frameworks and create a set of simplified, yet comprehensive, privacy management principles. Below are the seventeen (17) different frameworks the SCF Data Privacy Management Principles are mapped to:

- AICPA's Trust Services Criteria (TSC) SOC 2 (2017)
- Asia-Pacific Economic Cooperation (APEC)
- California Privacy Rights Act (CPRA)
- European Union General Data Protection Regulation (EU GDPR)
- Fair Information Practice Principles (FIPPs) - Department of Homeland Security (DHS)
- Fair Information Practice Principles (FIPPs) - Office of Management and Budget (OMB)
- Generally Accepted Privacy Principles (GAPP)
- HIPAA Privacy Rule
- ISO 27701
- ISO 29100
- Nevada SB820

[14] *SCF DPMP - https://securecontrolsframework.com/data-privacy-management-principles/*

- NIST SP 800-53 R4
- NIST SP 800-53 R5
- NIST Privacy Framework v1.0
- Organization for Economic Co-operation and Development (OECD)
- Office of Management and Budget (OMB) - Circular A-130
- Personal Information Protection and Electronic Documents Act (PIPEDA)

We took these frameworks and looked for similarities and also for gaps. If you download the SCF Data Privacy Management Principles, you will see the direct mapping to these leading privacy frameworks so you know the origin of the principle we include in our document. This will be a great tool for organizations that may have to address multiple requirements, since it brings a common language to simply things.

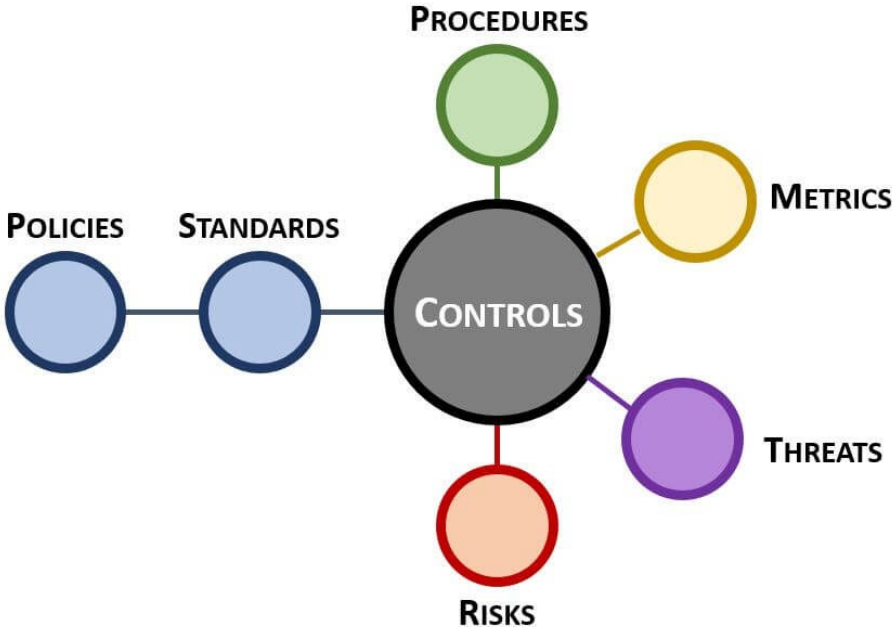
The eighty-six (86) principles of the SCF Data Privacy Management Principles are organized into eleven (11) domains:

1. Privacy by Design
2. Data Subject Participation
3. Limited Collection & Use
4. Transparency
5. Data Lifecycle Management
6. Data Subject Rights
7. Security by Design
8. Incident Response
9. Risk Management
10. Third-Party Management
11. Business Environment

Section 5: Integrated Controls Management (ICM) Approach To Using The SCF

The Integrated Controls Management (ICM) is a joint project between the SCF and ComplianceForge. The premise of the ICM is that controls are central to cybersecurity & data privacy operations, as well as the overall business rhythm of an organization. This is supported by the Cybersecurity & Data Privacy Risk Management Model (C|P-RMM), that describes the centralized nature of controls, where not just policies and standards map to controls, but procedures, metrics, threats and risks, as well.

ICM is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's cybersecurity & data privacy operations. ICM is designed to proactively address the strategic, operational and tactical nature of operating an organization's cybersecurity & data privacy program at the control level. ICM is designed to address both internal controls, as well as the broader concept of Supply Chain Risk Management (SCRM).



Applying ICM To Governance, Risk Management & Compliance (GRC) Functions

GRC can be a costly and labor-intensive endeavor, so what justifies the investment? Essentially, GRC functions help avoid negligence, with the added benefit of improved IT/cyber/privacy operating effectiveness. The reality of the situation is your company invests in cybersecurity & data privacy as a necessity. This necessity is driven in large part by laws, regulations and contractual requirements that it is legally obligated to comply with. It is also driven by the desire to protect its public image from damaging acts that happen when cybersecurity & data privacy practices are ignored. Regardless of the specific reason, those charged with developing, implementing and running your organization's cybersecurity and data protection program must do so in a reasonable manner that would withstand scrutiny that could take the form of an external auditor, regulator or prosecuting attorney.

How fast would you drive your car if you didn't have any brakes? Think about that for a moment - you would likely drive at a crawl in first gear and even then you would invariably have accidents as you bump into objects and other vehicles to slow down. Brakes on a vehicle actually allow you to drive fast, in addition to safely navigating dangers on the road!

While it is not the most flattering analogy, GRC is akin to the brakes on your car, where they enable a business' operations to go fast and avoid catastrophic accidents. Without those "brakes", an accident is a certainty! These brakes that enable a business' operations to stay within the guardrails are its cybersecurity policies, standards and procedures. These requirements constitute "reasonable practices" that the organization is required to implement and maintain to avoid being negligent.

GRC Is A Plan, Do, Check & Act (PDCA) Adventure – That Is A Concept That Should Be Embraced, Not Fought Against

GRC most often deals with legally-binding requirements, so it is important to understand that negligence is situationally-dependent. For example, an intoxicated driver who gets behind the wheel acting negligently. However, when sober, that same individual is a champion race car driver who is highly skilled and would not be considered incompetent in any regard. In this example, driving intoxicated constitutes a negligent act and shows that negligence has nothing to do with being incompetent. The point is to demonstrate that an organization can employ many highly-competent personnel, but even competent people can behave in a negligent manner. GRC fundamentally exists to help an organization avoid circumstances that could be construed as negligent acts.

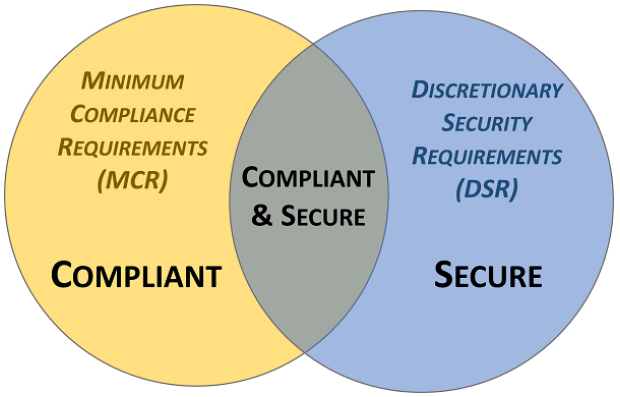
Considering how business practices continuously evolve, so must cybersecurity practices. The PDCA process (also referred to as the Deming Cycle) enables the GRC function to continuously evaluate risks, threats and performance trends, so that the organization's leadership can take the necessary steps to minimize risk by modifying how people, processes and technology work together to keep everything both secure and operational. The PDCA approach is a logical way to conceptualize how GRC works:

- **Plan**. The overall process beings with planning. At its core, this phase is the process of conducting due diligence. The results of this process will define necessary controls (e.g., requirements) that influence the need for policies, standards and procedures. These actions directly influence resourcing and procurement actions that range from staffing needs to tool purchases and services acquisition.
- **Do**. This phase is the process of conducting due care, where it is focused on the "reasonable care" necessary to properly and sufficiently conduct operations that demonstrate the absence of negligence. This is the execution of procedures – the processes that bring controls to life.
- **Check**. This phase can be considered maintaining situational awareness. There are several ways to maintain situation awareness and that ranges from control validation testing to audits/assessments and metrics.
- **Act**. This phase again brings up the concept of "reasonable care" that necessitates taking action to maintain the organization's targeted risk tolerance threshold. This deals with addressing two main concepts (1) real deficiencies that currently exist and (2) areas of concern that may expose the organization to a threat if no action is taken.

ICM Focuses On What It Means To Be "Secure & Compliant"

ICM specifically focuses on the need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, ICM helps an organization categorize its applicable controls according to "must have" vs "nice to have" requirements:

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.



Secure and compliant operations exist when both MCR and DSR are implemented and properly governed:

- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

The premise is that controls are central to cybersecurity & data privacy operations as well as the business rhythms of the organization. Without properly defining MCR and DSR thresholds, an organization's overall cybersecurity & data privacy program is placed in jeopardy as the baseline practices are not anchored to clear requirements. Furthermore, understanding and clarifying the difference between "compliant" versus "secure" (e.g., MCR only vs. MCR+DSR) enhances risk management discussions.

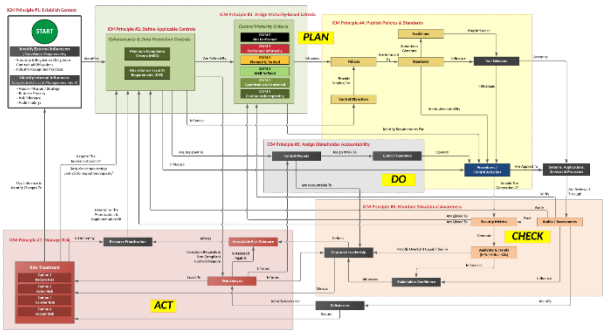
IT General Controls (ITGC)

The combination of MCR and DSR equate to an organization's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements for People, Processes, Technology & Data (PPTD) in one control set. It defines the Minimum Viable Product (MVP) technical and business requirements from a cybersecurity & data privacy perspective. In short, the MSR can be considered to be an organization's IT General Controls (ITGC), which establish the basic controls that must be applied to systems, applications, services, processes and data throughout the enterprise. ITGC provide the foundation of assurance for an organization's decision makers. ITGC enables an organization's governance function to define how technologies are designed, implemented and operated.

ICM Principles

There are eight (8) principles associated with ICM:

1. Establish Context
2. Define Applicable Controls
3. Assign Maturity-Based Criteria
4. Publish Policies, Standards & Procedures
5. Assign Stakeholder Accountability
6. Maintain Situational Awareness
7. Manage Risk
8. Evolve Processes



[graphic can be downloaded from https://complianceforge.com/content/Plan-Do-Check-Act.pdf]

Principle 1: Establish Context

To build and maintain efficient and effective operations, a cybersecurity & data privacy program must have a hierarchical vision, mission and strategy that directly supports the organization's broader strategic objectives and business processes. This process of establishing context involves identifying all applicable external compliance requirements (e.g., laws, regulations and contractual obligations), as well as internal directives (e.g., Board of Directors, corporate policies, etc.). This is a due diligence element of the cybersecurity & data privacy program.

Principles 2: Define Applicable Controls

A tailored control set cybersecurity and data protection controls must exist. This control set needs to be made of Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (DSR). This blend of "must have" and "nice to have" requirements establish an organization's tailored control set to ensure both secure practices and compliance.

Principle 3: Assign Maturity-Based Criteria

The cybersecurity & data privacy program must assign maturity targets to define organization-specific "what right looks like" for controls. This establishes attainable criteria for people, processes and technology requirements. Tailored maturity level criteria can be used to plan for, budget for and assess against. Maturity targets should support the organization's need for operational resiliency.

Principle 4: Publish Policies, Standards & Procedures

Documentation must exist, otherwise an organization's cybersecurity and data protection practices are unenforceable. Formalizing organization-specific requirements via policies and standards are necessary to operationalize controls. Documented policies and standards provide evidence of due diligence that the organization identified and implemented reasonable steps to address its applicable requirements.

Principle 5: Assign Stakeholder Accountability

Controls must be assigned to stakeholders to ensure accountability (e.g., business units, teams and/or individuals). These "control owners" may assign the task of executing controls to "control operators" at the Individual Contributors (IC)-level. Stakeholders utilize the prescriptive requirements from policies and standards to develop Standardized Operating Procedures (SOP) that enable ICs to execute those controls. The documented execution of procedures provides evidence of due care that reasonable practices are being performed.

Principle 6: Maintain Situational Awareness

Situational awareness must involve more than merely "monitoring controls" (e.g., metrics). While metrics are a point-in-time

snapshot into discrete controls' performance, the broader view of metrics leads to a longer-term trend analysis. When properly tied in with current risk, threat and vulnerability information, this insight provides "situational awareness" that is necessary for organizational leadership to adjust plans to operate within the organization's risk threshold.

PRINCIPLE 7: MANAGE RISK

Proactive risk management processes must exist across all phases of development/information/system life cycles to address confidentiality, integrity, availability and safety aspects. Risk management must address internal and external factors, including privacy and Supply Chain Risk Management (SCRM) considerations. To manage risk, it requires the organization to enforce a clearly defined risk threshold and ensure reasonable security practices are operational.

PRINCIPLE 8: EVOLVE PROCESSES

Cybersecurity and data protection measures must adapt and evolve to address business operations and the evolving threat landscape. This requires the adoption of a Plan, Do, Check & Act (PDCA) approach (Deming Cycle) to ensure the organization proactively identifies its requirements, implements appropriate protections, maintains situational awareness to detect incidents, operates a viable capability to respond to incidents and can sustain key business operations, if an incident occurs.

SECTION 6: PRACTICAL APPROACH TO USING THE SCF TO IMPLEMENT ICM

ICM is meant to be put into practice by organizations of any size or industry. The information below provides an understanding of available options to implement ICM with existing solutions. The SCF is a great way to implement the ICM.

STEP 1: ESTABLISH CONTEXT

Part of your due diligence process is to establish the context of the scope for cybersecurity & data privacy controls. Practical steps to establish context includes:

- Read through the C|P principles to familiarize yourself with the 32 domains to understand how they come together to address the cybersecurity, privacy and physical security considerations for a modern security program.
- Talk with representatives outside of IT and cybersecurity to gain an appreciation of other compliance requirements (e.g., legal, procurement, physical security, etc.).
- Come up with a list of the "must have" laws, regulations and frameworks that your organization must comply with.
- Come up with a list of "nice to have" requirements that your Board of Directors, or other stakeholders, feel are necessary.

Understanding the requirements for both cybersecurity & data privacy principles involves a simple process of distilling expectations. This process is all part of documenting reasonable expectations that are "right-sized" for an organization, since every organization has unique requirements.

Some people freak out and think they have to do all 1,000+ controls in the SCF and that is just not the case. It is best to visualize the SCF as a "buffet of cybersecurity & data privacy controls," where there is a selection of 1,000+ controls available to you. You as you do not eat everything possible on a buffet table, the same applies to the SCF's control set. Once you know what is applicable to you, you can generate a customized control set that gives you just the controls you need to address your statutory, regulatory and contractual obligations.

The approach looks at the following spheres of influence to identify applicable SCF controls:

- Statutory obligations - These are laws (e.g., US state, federal and international laws).
- Regulatory obligations - These are requirements from regulatory bodies or governmental agencies.
- Contractual obligations - These are requirements that are stipulated in contracts, vendor agreements, etc.
- Industry-recognized practices - These are requirements that are based on an organization's specific industry that are considered reasonably-expected practices.

Please keep in mind that the SCF is a tool and it is only as good as its used – just like a pocketknife shouldn't be used as a prybar. Realistically, if you do not scope the controls from the SCF correctly, you will not address your applicable compliance requirements since you are missing what is expected. That is not a deficiency of the SCF – that is simply negligence on the part of the user of the tool.

To make sure scoping is done properly, it is imperative for you to speak with your legal, IT, project management, cybersecurity and procurement teams (and other stakeholders you may feel are relevant to scoping controls). The reason for this collaboration is so that you can get a complete picture of all the applicable laws, regulations and frameworks that your organization is legally obligated to comply with. Those teams will likely provide the best insights into what is required and that list of requirements will then make it simple to go through and customize the SCF for your specific needs!

STEP 2: DEFINE APPLICABLE CYBERSECURITY & DATA PRIVACY CONTROLS (TAILOR THE SCF)

There is a column that exists in the SCF to help with the task of defining applicable controls. It is a column called the "Minimum Security Requirements (MSR) Filter" that will assist you in this process.

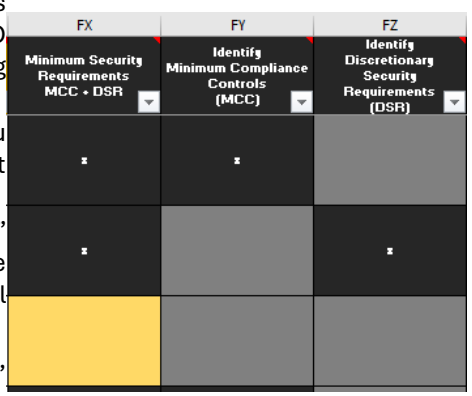
The SCF is fundamentally an Excel spreadsheet. Therefore, you can use your Excel skills to manually filter the requirements. If you are comfortable with Excel, it might take you 5-10 minutes to do this filtering, based on how many requirements you need to map to.

As previously mentioned, the ICM is focused on defining "must have" vs "nice to have" requirements:

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.
- Minimum Security Requirements (MSR) is the resulting set of controls necessary to be "compliant and secure" to manage

your organization's cybersecurity & data privacy program.

Follow these steps to tailor the SCF:

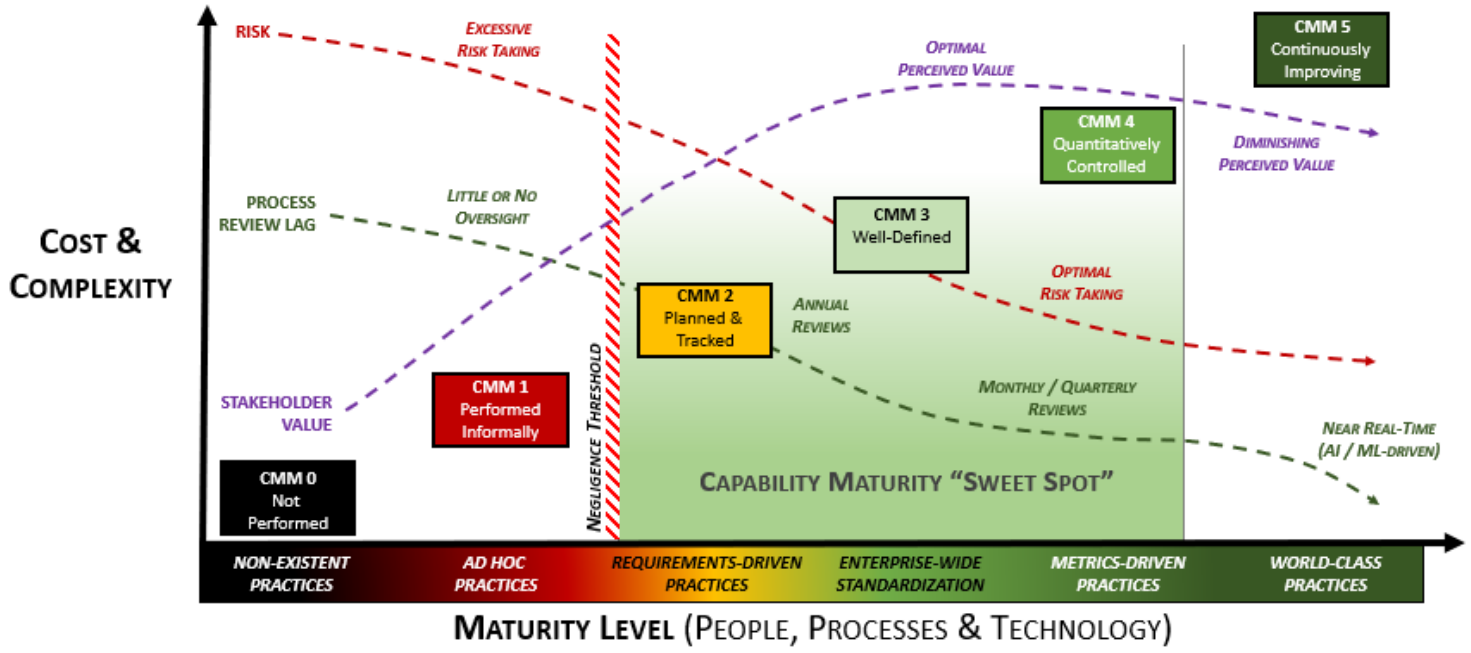


1. Either hide or delete all of the columns containing laws, regulations or frameworks that are not applicable to your organization (e.g., if you only have to comply with ISO 27002, PCI DSS and EU GDPR, then you can delete or hide all other mapping columns but those).
2. Using the filter option in Excel (little gray arrow on the top row in each column), you would then filter the columns to only show cells that contain content (e.g., don't show blank cells in that column).
3. In that MCR column, simply put an "x" to mark that control as being "must have" controls. In the DSR column, simply put an "x" to mark that control as being "nice to have" controls. A selection of either MCR or DSR will select MSR. Do this for all the rows shown in that column.
4. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
5. Repeat step 3 and step 4 until all your applicable laws and regulations are mapped to.
6. The MSR column will now have an "x" that marks each SCF control that is applicable for your needs, based on what was selected for MCR and DSR controls.

This will leave you with a SCF control set that is tailored for your specific needs.

STEP 3: DEFINE ORGANIZATION-SPECIFIC MATURITY CRITERIA AT THE CONTROL OR DOMAIN LEVEL

From the previous step, you identified the controls that are applicable to your specific needs (e.g., MCR + DSR). You can now use the SP- CMM criteria to "define what right looks like" for each control. This is further explained in the Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM).[15]



Negligence Considerations

Without the ability to demonstrate evidence of both due care and due diligence, an organization may be found negligent. In practical terms, the "negligence threshold" is between C|P-CMM 1 and C|P-CMM 2. The reason for this is at C|P-CMM 2, practices are formalized to the point that documented evidence exists to demonstrate reasonable steps were taken to operate a control.

Risk Considerations

[15] *SCF C|P-CMM - https://securecontrolsframework.com/capability-maturity-model/*

Risk associated with the control in question decreases with maturity, but noticeable risk reductions are harder to attain above C|P-CMM 3. Oversight and process automation can decrease risk, but generally not as noticeably as steps taken to attain C|P-CMM 3.

Process Review Lag Considerations

Process improvements increase with maturity, based on shorter review cycles and increased process oversight. What might have been an annual review cycle to evaluate and tweak a process can be near real-time with Artificial Intelligence (AI) and Machine Learning (ML).

Stakeholder Value Considerations

The perceived value of security controls increases with maturity. However, perceived value tends to decrease after C|P-CMM 3 since the value of the additional cost and complexity becomes harder to justify to business stakeholders. Companies that are genuinely focused on being industry leaders are ideal candidates for C|P-CMM 5 targets to support their aggressive business model needs.

The C|P-CMM draws upon the high-level structure of the **Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM)**, since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the SSE-CMM Model Description Document that is hosted by the US Defense Technical Information Center (DTIC).

Note: The SCF will not tell you what you should select, since that is a due diligence step that you have to address, based on the risk tolerance that your organization is willing to accept.

STEP 4: PUBLISH CYBERSECURITY & DATA PRIVACY POLICIES, STANDARDS & PROCEDURES

There are generally three (3) options to obtain cybersecurity & data privacy documentation:

1. Use internal resources to write it in-house;
2. Hire a consultant to write a bespoke set of documentation; or
3. Purchase semi-customized templates online.

ComplianceForge wrote a document to help organizations understand cybersecurity & data privacy documentation. This guide is a free resource to educate organizations on proper cybersecurity and data protection documentation, based on definitions from authoritative sources. These policies and standards provide the requirements that your organization has to adhere to.[16]

STEP 5: IDENTIFY STAKEHOLDERS & ASSIGN ACCOUNTABILITY FOR CONTROLS

Assigning stakeholder accountability offers unique challenges for organizations, since it is beyond IT, cybersecurity & data privacy. Common stakeholders involve Human Resources (HR), procurement, facilities management, legal and many other teams to ensure accountability is enforceable. Realistically, this step is an executive-management function since it requires inter-departmental enforcement by organizational management.

A great starting point is the NIST SP 800-181, Workforce Framework for Cybersecurity (NICE Framework).[17] The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.

STEP 6: MAINTAIN SITUATIONAL AWARENESS THROUGH METRICS & ANALYTICS

Maintaining situational awareness has different meanings, based on the security culture of an organization. For some organizations, it means metrics, while for others it means a broader understanding of control performance, risks, threats and current vulnerability information.

The ComplianceForge Security Metrics Reporting Model™ (SMRM) takes a practical view towards implementing a sustainable metrics reporting capability.[18] At the end of the day, executive management (e.g., CIO, CEO, Board of Directors (BoD), etc.) often just want a simple answer to a relatively-straightforward question: "Are we secure?"

---

[16] *ComplianceForge Guide To Understanding Cybersecurity & Data Privacy Documentation - https://complianceforge.com/content/Understanding-Cybersecurity-Data-Privacy-Documentation.pdf*

[17] *NIST SP 800-181 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf*

[18] *Cybersecurity Metrics Reporting Model (CMRM) - https://complianceforge.com/content/graphics/Cybersecurity-Metrics-Reporting-Model.pdf*

In order for a CISO to honestly provide an answer, it requires a way for the CISO to measure and quantify an "apples and oranges" landscape where processes and technologies lack both uniform risk weighting and abilities to capture metrics.

STEP 7: MANAGE RISK

There are many ways to manage risk. However, the SCF's Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) contains a control-centric:[19]

- Risk catalog;
- Threat catalog; and
- Methodology to not only perform a risk assessment, but manage risk across the organization.

The value of the C|P-RMM is having a standardized methodology where controls are tied to specific risks and threats. Based on the other criteria offered by the SCF (e.g., weighting and maturity criteria), the C|P-RMM makes calculating risk a straightforward process.

Controls are the nexus of a cybersecurity & data privacy program, so it is vitally important to understand how controls should be viewed from a high-level risk management perspective. To progress from identifying a necessary control to a determination of risk, it is a journey that has several steps, each with its own unique terminology. Therefore, it is important to baseline the understanding of risk management terminology.

Traditional risk management practices have four (4) options to address identified risk:

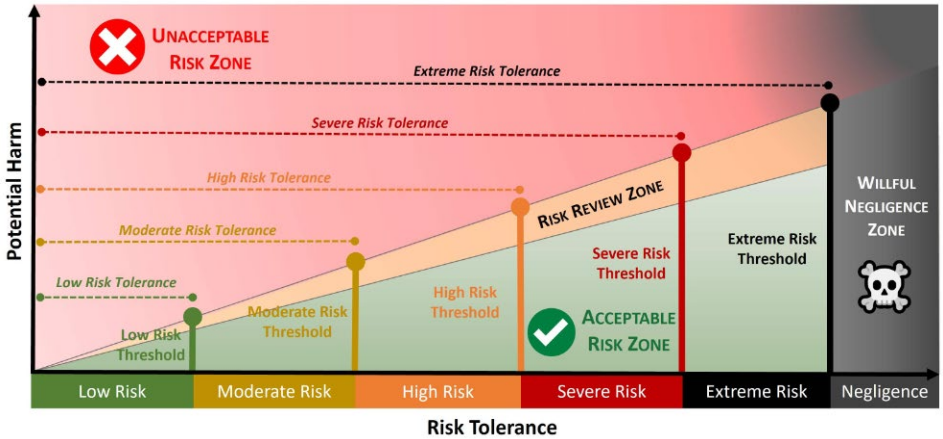
1. Reduce the risk to an acceptable level;
2. Avoid the risk;
3. Transfer the risk to another party; or
4. Accept the risk.

In a mature risk program, the results of risk assessments are evaluated with the organization's risk appetite into consideration. For example, if the organization has a Moderate Risk Appetite and there are several findings in a risk assessment that are High Risk, then action must be taken to reduce the risk. Accepting a High Risk would violate the Moderate Risk Appetite set by management. In reality, which leaves remediation, transferring or avoiding as the remaining three (3) options, since accepting the risk would be prohibited.

Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an organization to unnecessary peril.

The goal of risk analysis is to determine the potential negative implications of an action or situation to determine one (1) of two (2) decisions:

1. **Acceptable Risk**: the criteria fall within a range of acceptable parameters; or
2. **Unacceptable Risk**: The criteria fall outside a range of acceptable parameters.



[19] *SCF C|P-RMM - https://securecontrolsframework.com/risk-management-model/*

STEP 8: IMPLEMENT PRACTICES TO CONTINUOUSLY IMPROVE & EVOLVE PROCESSES

The ComplianceForge Integrated Cybersecurity Governance Model™ (ICGM) takes a comprehensive view towards governing a cybersecurity & data privacy program.[20] Without an overarching concept of operations for the broader GRC/IRM function, organizations will often find that their governance, risk management, compliance and privacy teams are siloed in how they think and operate. These siloed functions and unclear roles often stem from a lack of a strategic understanding of how these specific functions come together to build a symbiotic working relationship between the individual teams that enables quality control over people, processes and technology.

The ICGM utilizes a Plan, Do, Check & Act (PDCA) approach that is a logical way to design a governance structure:

- Plan. The overall ICM process beings with planning. This planning will define the policies, standards and controls for the organization. It will also directly influence the tools and services that an organization purchases, since technology purchases should address needs that are defined by policies and standards.
- Do. Arguably, this is the most important section for cybersecurity & data privacy practitioners. Controls are the "security glue" that make processes, applications, systems and services secure. Procedures (also referred to as control activities) are the processes in which the controls are actually implemented and performed.
- Check. In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.
- Act. This is essentially risk management, which is an encompassing area that deals with addressing two main concepts (1) real deficiencies that currently exist and (2) possible threats to the organization.

[20] *Integrated Cybersecurity Governance Model (ICGM) - https://complianceforge.com/content/Plan-Do-Check-Act.pdf*